DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

SECNAVINST 5239.3A
DON CIO
20 December 2004

SECNAV INSTRUCTION 5239.3A

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY INFORMATION ASSURANCE (IA) POLICY

Ref:
(a) Federal Information Security Management Act of 2002, Title III of E-Government Act of 2002 (PL 107-347)
(b) CNSS Instruction 4009, National Information Systems Security Glossary, May 2003
(c) DoDD 8500.1, Information Assurance (IA), 24 Oct 2002
(d) DoDI 8500.2, Information Assurance (IA) Implementation, 2 Jun 2003
(e) DoDD 5000.1, The Defense Acquisition System, 12 May 2003
(f) DoDI 5000.2, Operation of the Defense Acquisition System, 12 May 2003
(g) Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, 17 Dec 2003
(h) NSTISSD 500, Information Systems Security Education, Training, and Awareness, 25 Feb 1993
(i) NSTISSI 4011, National Training Standard for Information Systems Security Professionals, 20 Jun 1994
(j) NSTISSI No. 4012, National Training Standard for Designated Approving Authority, Aug 1997
(k) DoDD 8570.1, Information Assurance Training, Certification, and Workforce Management, 15 Aug 2004
(l) SECNAV 5211.5D, DON Privacy Act Program, 17 July 1992
(m) SECNAVINST 5720.47, Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites
(n) DoDD 5200.2, DoD Personnel Security Program, 4 Sep 1999
(o) DoD 5200.2-R, Personnel Security Program
(p) DoDD 5230.20, Visits, Assignments, and Exchanges of Foreign Nationals, 12 Aug 1998
(q) DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations

(r) Department of the Navy Chief Information Officer (DON CIO) Guidance On Information Management/Information Technology Inherently Governmental Functions, Nov 2001 (NOTAL)
(s) DoDD O-8530.1, Computer Network Defense (CND), 8 Jan 2001 (NOTAL)
(t) DoDI O-8530.2, Support to Computer Network Defense, 3 Sep 2001 (NOTAL)
(u) DoD CIO Memorandum of 7 Nov 2000, Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems (NOTAL)
(v) DoDD 8190.3, Smart Card Technology, 31 Aug 2002
(w) DoDI 8520.2, Public Key Infrastructure (PKI) and Public key (PK) Enabling, 1 Apr 2004
(x) OMB Circular A-130, Management of Federal Information Resources, 28 Nov 2000 (NOTAL)
(y) DoDD 3020.26, Continuity of Operations (COOP) Policy and Planning, 26 May 1995
(z) DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004
(aa) DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 1997
(ab) DCI Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems, 5 June 1999
(ac) DoDD C-5200.5, Communications Security (COMSEC) (U), 21 Apr 2000 (NOTAL)
(ad) DoD 5220.22-M, National Industrial Security Program Operating Manual, Jan 1995
(ae) OMB Circular A-11, Preparation, Execution, and Submission of the Budget, July 2003 (NOTAL)
(af) OMB Memo M-00-07, Incorporating and Funding Security in Information Systems Investments, 28 Feb 2000 (NOTAL)

Encl: (1) List of Acronyms
(2) Reference Location Table

1. Purpose

a. To establish Information Assurance (IA) policy for the Department of the Navy (DON) consistent with National and Department of Defense (DoD) policies.

b. To designate the DON Chief Information Officer (DON CIO) as the Department of the Navy official assigned responsibility, and delegated authority, in accordance with reference (a), to ensure requirements contained in reference (a), the Federal Information Security Management Act (FISMA), are carried out by the Department of the Navy.

c. To assign responsibilities within the DON for the development, implementation, management, and evaluation of DON IA programs, policies, procedures and controls.

2. Cancellation. SECNAVINST 5239.3. This instruction is a complete revision and should be reviewed in its entirety.

3. Acronyms, Definitions, and References. Acronyms used in this instruction are defined in enclosure (1). Definitions are listed in references (b), (c), and (d). Enclosure (2) lists the sources for references.

4. Objectives

a. To establish within the Department of the Navy an IA policy that provides information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access to, use, disclosure, disruption, modification or destruction of:

(1) Information collected or maintained by or on behalf of the Department of the Navy; and

(2) Information Systems used or operated by the Department of the Navy, by a contractor of the Department of the Navy processing DON information, or other organizations on behalf of the Department of the Navy.

b. To establish within the Department those measures necessary to protect the availability, integrity, authentication, confidentiality, and non-repudiation of Information Technology (IT) assets. These measures will include the capability to detect and react to attacks and intrusions, mitigate the effects of incidents, support the restoration of

services, and perform post-incident analysis. These measures are based on mission criticality, required level of assurance, and classification or sensitivity of information processed, stored, and/or transmitted.

c. To ensure all personnel who use or support DON Information Systems (IS) receive IA training commensurate with their duties.

d. To maintain the DON consistent with comprehensive DoD-wide approaches for protection of IT resources and systems as defined in National and DoD policy.

e. To incorporate IA as a critical component of the life cycle management process.

f. To require that DON IT systems are registered in the DON IT Registration Database in accordance with references (e) and (f) and periodic DON IT Registration Database guidance issued by DON CIO.

g. To require that all IT systems under DON authority that require certification and accreditation (C&A) are certified and accredited.

h. To ensure that IA-related technology research and development efforts are responsive to the IA needs of the DON.

i. To require DON IA policies and procedures to be reviewed on an annual basis to ensure effectiveness, as required by reference (a).

j. To ensure all DON IT expenditures clearly reflect security considerations.

5. Scope

a. This instruction applies to:

(1) The Department of the Navy.

(2) All DON owned or controlled information systems that

receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity.

b. Nothing in this policy shall alter or supercede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence.

6. Background. Per references (a) and (c), IA provides the measures taken by an organization to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of its information and information systems. IA includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Systems Security (INFOSEC), a subset of IA, is the protection of information and information systems against unauthorized access or modification, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Defense-in-depth is the DON-preferred security strategy whereby layers of protection establish an adequate security posture for a system. The strategy is based on the concept that attacks that must penetrate multiple protection layers of the system are less likely to be successful. In addition to this layered approach, protection mechanisms are distributed among multiple locations, and each component of defense within the system provides an appropriate level of robustness. Management of risk is the objective of IA in a defense-in-depth strategy.

Computer Network Defense (CND) embodies incident detection and response, a critical part of defense-in-depth. CND synchronizes the technical, operational, and intelligence assessments of the nature of a computer attack in order to defend against it. The Joint Task Force for Global Network Operations (JTF-GNO), under US Strategic Command, is the lead organization designated to identify and mitigate threats to the DoD information networks, and to direct the defense of the

Global Information Grid (GIG). The Naval Computer Incident Response Team (NAVCIRT) and Marine Corps Network Operations and Security Command (MCNOSC) report incidents and associated analytical results to the JTF-GNO. The Naval Criminal Investigative Service maintains investigative authority for criminal acts or espionage related to computer network security incidents, and coordinates information regarding these incidents with the Law Enforcement Counterintelligence Center, a part of the JTF-GNO, for the purpose of preventing future attacks.

7. Policy

a. Precedence. This policy is consistent with Federal and DoD IA and Critical Infrastructure Protection (CIP) policies, the latter established from reference (g). In case of a conflict with other policies, policy and requirements set forth by higher authority take precedence over the policy established in this instruction. Implementing authorities should identify conflicting policy to DON CIO for resolution.

b. Training. All personnel, commensurate with their responsibilities, shall receive IA training that meets the requirements set forth in references (c), (d), and (h) through (j) as appropriate. Reference (k) requires all personnel who access DON Information and Information Systems receive annual IA and Security Awareness Training, to include emphasis on Internet security. This training shall ensure all personnel are aware of best security practices, the information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. Reference (k) also requires that all personnel with privileged access to DON information systems and networks, and Designated Approving Authorities (DAAs), shall receive training and be certified for their position.

c. Defense-in-Depth. Commanders, commanding officers, officers in charge, and directors, hereinafter referred to as Commanders of DON organizations, shall, in their role as local IA authorities, implement a DoD defense-in-depth IA strategy to mitigate information security risks. Except where otherwise indicated, references (c) and (d) provide guidance for establishing and implementing defense-in-depth measures which shall, at a minimum, include the following:

(1) Boundary Defense. Commanders of DON organizations shall use boundary protection mechanisms to limit access to internal networks. These mechanisms may include, but are not limited to routers, firewalls, intrusion detection systems, and NSA-approved cross-domain solutions. Generally, the amount of protection provided should be increased as the sensitivity of the information increases, as the threat increases, and as the operational environment changes (e.g. likelihood for attack increases for high profile organizations).

(2) Access Control. Commanders of DON organizations shall control internal and external access to their information systems.

(a) Connection. Commanders of DON organizations shall obtain formal authorization to interconnect information systems in accordance with references (c) and (d).

(b) Privileged Users. Commanders of DON organizations functioning as Information System Owners shall designate in writing Information Assurance Managers (IAM), Information Assurance Officers (IAO), and all personnel with privileged access, in accordance with reference (d).

(c) Remote Access. Commanders of DON organizations shall control remote access to DON information systems in accordance with reference (d). For telework, the preferred method for access is via a Government-owned computer.

(d) Security and Privacy Notices. All DON information systems and web sites shall display the appropriate privacy policy in accordance with reference (l) and the official DoD security banner in accordance with reference (m).

(e) The Insider Threat. The insider security threats (whether intentional or unintentional) are potentially more serious than the external threat because perpetrators of malicious activity or inadvertent mistakes do not have to penetrate multiple layers of defense and may have authorized access to systems. Commanders of DON organizations shall be aware of the insider threat and plan risk mitigation strategies that involve people, processes, and technology.

(f) Access by Foreign Nationals. The Assistant for Administration, Office of the Under Secretary of the Navy (AA/USN) and/or the Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) shall control access by foreign nationals to DON systems in accordance with relevant national and DoD level policies and guidance including references (c), (d), (n), (o), (p), and (q). AAUSN, CNO, and CMC may delegate this authority only as long as they comply with the applicable policies of reference (c), including:

1. Policies and procedures are in place to sanitize or reconfigure DON information systems to prevent unauthorized access to classified and controlled unclassified information by foreign nationals.

2. Foreign nationals are identified in all network communications, including e-mail.

(3) Inherently Governmental Functions. In accordance with reference (r), commanders of DON organizations shall not assign contractor personnel to inherently governmental IA functions.

(4) Intrusion Detection Systems and Incident Response. The goal of an intrusion detection system (IDS) is to detect and identify unauthorized use, misuse, and abuse of computer systems by both internal network users and external attackers in "near real time." DON organizations shall establish structured capabilities to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of DON operations. All DON organizations shall report computer incidents in accordance with references (s) and (t).

(5) Malicious Mobile Code/Virus Detection and Neutralization. Malicious mobile code is software transferred from remote systems (normally outside the enclave boundary), then downloaded and executed on a local system without explicit installation or execution by the recipient. To protect DON systems from malicious or improper use of mobile code, commanders of DON organizations shall assess and mitigate the risks of this technology in accordance with reference (u), and:

(a) Ensure that anti-virus protection mechanisms are installed on all IT systems and that these mechanisms are

updated regularly. Anti-virus system settings should perform these updates automatically, reliably, and through a centrally controlled management framework, where feasible.

(b) Report malicious code outbreaks to the appropriate combatant commander and to the Naval Computer Incident Response Team (NAVCIRT) or MCNOSC in accordance with references (s) and (t).

(6) Virtual Private Networks. Commanders of DON organizations shall consider the use of virtual private networks (VPN) to protect and control internal and external access to their IT systems. Administrators' access to IT systems from outside the enclave must use VPN connections. VPNs help to ensure that network services provide appropriate confidentiality and integrity of information.

(7) Public Key Infrastructure. Commanders of DON organizations shall continue to aggressively implement the DoD Public Key Infrastructure (PKI), in concert with adopting the Common Access Card (CAC), in accordance with references (d), (s), (t), (v), and (w). PKI provides digital identification, signature, and encryption services to a broad range of applications at various levels of assurance. PKI is an enabling technology that will reduce access management administration while increasing overall security and access control.

(8) Internet Security. Commanders of DON organizations shall manage all interconnections of DON information systems, both internal and external, to minimize community risk. Physical or technical means, such as an approved boundary protection product, shall be used to protect DON information systems that allow open, unrestricted access to the public, or systems that allow unrestricted access to and from the Internet. Whenever appropriate, DON organizations shall give preference to DoD-owned or -controlled (including by a DOD contractor) web servers rather than commercial web servers to further minimize exposure and enhance operational security by limiting data aggregation opportunities. All DON private web servers shall be issued DoD PKI server certificates and shall use the certificates for server authentication via the Secure Sockets Layer (SSL) protocol. Additionally, all DON information systems

and web sites shall display the appropriate official notifications for security and privacy. DON website developers shall adhere to reference (m).

(9) Physical Security. Commanders of DON organizations shall act to ensure the protection of DON information technology resources (e.g., installations, personnel, equipment, electronic media, documents, etc.) from damage due to malicious activities, natural disasters, loss, theft, or unauthorized physical access.

(10) Contingency Planning/Continuity of Operations Planning. Commanders of DON organizations shall develop and test contingency plans in accordance with references (x) and (y) to prepare for emergency response, backup operations, and post-disaster recovery. Contingency plans shall as a minimum:

(a) Identify critical physical and cyber infrastructures and assess the risk of loss of service availability.

(b) Provide for continued operational availability of these identified systems by describing: risk mitigation, response to attempts to deny system availability, and reconstitution of the system should availability be denied.

(c) Be evaluated in the system’s System Security Authorization Agreement (SSAA).

(11) Information Operations Conditions. To ensure adequate incident response, commanders of DON organizations shall develop, implement, and manage Information Operations Conditions (INFOCON) as required in references (s) and (t). Although higher authority normally prescribes INFOCONs, local commanders have the authority to increase INFOCONs within their area of responsibility when the circumstances dictate. This increased security posture is one more tool at the commander’s disposal in the defense-in-depth architecture.

(12) Mission Assurance Categories. In accordance with reference (c), DAAs shall require the assignment of a Mission Assurance Category (MAC) to each DON information system. The Mission Assurance Category is directly associated with the

importance of the information the system contains relative to the achievement of DON goals and objectives, particularly the warfighter mission. Requirements for availability and integrity are associated with the Mission Assurance Category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are tenets of defense-in-depth.

d. Acquisition Management. DON organizations shall implement a defense-in-depth strategy throughout the life cycle of the system. This applies to all DON information systems used to enter, process, store, display, or transmit information.

(1) In accordance with reference (f), DON organizations shall not award a contract for the acquisition of a mission-critical or mission-essential IT system until the system is registered in the DON IT Registration Database. Further, acquisition programs require an Acquisition IA Strategy if they are designated Mission Critical or Mission Essential.

(2) In accordance with reference (z), DON organizations shall ensure that IA is fully integrated into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, and operation. This requirement includes:

(a) Appointment of an IA Manager.

(b) Determination of a system Mission Assurance Category and confidentiality level.

(c) Planning and execution of the certification and accreditation process in accordance with references (aa) or (ab) as appropriate.

(3) DON organizations shall acquire and utilize National Information Assurance Partnership (NIAP) evaluated or validated Government-off-the-Shelf (GOTS) or Commercial-off-the-Shelf (COTS) IA and IA-enabled IT products for all IT systems in accordance with reference (d).

(4) The DON shall acquire communications security (COMSEC) products and services to protect classified systems

through the National Security Agency (NSA) or NSA-designated agents per reference (ac).

(5) DON organizations shall include requirements to protect classified and sensitive unclassified information in contracts and monitor contractors for compliance in accordance with references (d), (e), (f), and (ad).

(6) Commanders of DON organizations shall assess the risk of allowing foreign nationals to compose code for and/or access Navy information systems, in accordance with references (c) and (d). The result of the risk assessment shall guide access restrictions and security requirements for the contract.

(7) Commanders of DON organizations shall implement those steps necessary to ensure acquisition managers address IA requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and IT programs that depend on external information sources or provide information to other DoD systems, in accordance with references (c), (d), (e) and (f).

e. Certification and Accreditation (C&A). References (c) and (d) require certification and accreditation of DON information systems in accordance with references (aa) or (ab), as appropriate, with the exception of platform IT with no network interconnection to the Global Information Grid. Further, references (c) and (d) mandate the assignment of a DAA for each DoD IT information system.

(1) Certification is the comprehensive evaluation of the technical and non-technical security features of an information system, and other safeguards to establish the extent that a particular design and implementation meets a set of specified security requirements. The certification process should result in a recommendation to the DAA for a risk mitigation decision and future accreditation.

(2) Accreditation is the formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

(3) The DAA has formal responsibility for the secure operation of information systems within his/her area of responsibility. The appropriate DAA shall formally approve a system to operate when an acceptable level of risk has been achieved through application of appropriate risk mitigation. DAAs shall accredit DON information systems that meet the requirements of references (c) and (d) in accordance with the C&A process.

f. Plans of Action and Milestones (POA&M). DON organizations shall develop POA&Ms to delineate the tasks and schedule necessary to successfully achieve system certification and accreditation. The purpose of the POA&M is to assist DON organizations in identifying, assessing, prioritizing, and monitoring the progress to C&A programs and systems. POA&Ms are especially important for non-accredited systems for which a Capital Asset Plan and Business Case (Exhibit 300) is submitted in accordance with reference (ae).

g. Information Assurance Vulnerability Management Process. The Information Assurance Vulnerability Management (IAVM) process is designed to provide positive control of the vulnerability notification and corrective action process within DoD. DON organizations shall comply with the IAVM process in accordance with references (s) and (t).

h. Research and Development. DON shall leverage commercial IA technology in conjunction with available government IA technology. The DON shall deploy IA solutions that support full interoperability and integration of IT activities across DoD.

8. Responsibilities

a. The Department of the Navy Chief Information Officer (DON CIO) shall:

(1) Carry out for the Secretary of the Navy the information assurance responsibilities assigned in reference (a) to the Head of each Federal Agency. Accordingly, the DON CIO shall ensure DON compliance with the information assurance requirements of references (a), (c), and (d) and related IA policies, procedures, standards and guidelines.

(2) Develop information security policies sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the DON.

(3) Designate a Senior DON Information Assurance Officer who shall report to the CIO on DON IA information assurance policies in accordance with reference (a). This action meets the requirements of section 3544.(a)(3) of reference (a).

(4) Ensure senior DON officials provide IA protections for DON information and information systems that support the operations and assets under their control. These IA protections include assessment, determining appropriate levels of information assurance, implementing policies and procedures to cost-effectively reduce risks to an acceptable level, and periodically testing and evaluating IA controls and techniques to ensure effective implementation.

(5) Set DON IA policy for personnel education, training, and awareness, commensurate with their respective responsibilities regarding information and information systems, and including Internet security and DAA training.

(6) Develop a DON IA strategy to provide information security for the operations and assets of the DON.

(7) Integrate IA requirements with DON strategic and operational planning, and into the DON major system acquisition management process.

(8) Serve as the focal point to ensure coordination of issues with other military departments, defense agencies, and DoD.

(9) Evaluate annually the effectiveness of the DON IA program in accordance with reference (a) and provide input to the DoD CIO for a collective report on information security.

(10) Set policy and procedures to control access by foreign nationals to information and information systems owned by the DON, in accordance with references (c), (d), (n), (o), (p), and (q).

(11) Require use of standard formats specified in reference (d) to identify foreign nationals and contractors in all forms of communications owned and operated by the DON, including e-mail, in accordance with reference (c).

(12) Coordinate with the Auditor General of the Navy for recommendations for IA audits and reviews.

(13) Review IA strategies for major defense acquisition programs and major automated information systems in accordance with reference (f) as part of the process for managing IT investments.

(14) Report annually, in coordination with other senior officials, to the Secretary of the Navy on the effectiveness of the DON IA program, including progress on remedial actions.

b. The DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) shall, subject to the authority of the DON CIO, implement and enforce policies, standards, and procedures to ensure that the DON complies with applicable statutes, regulations, and directives.

c. The Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RD&A)) shall:

(1) Issue DON acquisition policies providing implementation details and procedures to support IA.

(2) Integrate IA requirements into acquisition management of all DON IT systems throughout their life cycle in accordance with reference (d).

(3) Maintain a robust and relevant science and technology (S&T) program in information assurance, in accordance with reference (a).

d. The Assistant for Administration, Office of the Under Secretary of the Navy (AA/USN) shall:

(1) Function as DAA for Secretariat systems.

(2) Set policies and procedures to control access by foreign nationals to information and information systems owned or operated at the SECNAV level, in accordance with references (c), (d), (n), (o), (p), and (q).

(3) Implement standard formats specified in reference (d) to identify foreign nationals and contractors in all forms of communications owned and operated at the SECNAV level, including e-mail, in accordance with reference (c).

e. The Chief of Naval Operations (CNO) shall:

(1) Ensure the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems supporting Navy operations and assets.

(2) Develop and implement information assurance programs, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the Navy. The Navy IA programs shall contain the elements of a DoD Component IA Program as specified in enclosure (3) to reference (d).

(3) Ensure that information assurance is practiced throughout the life cycle of each Navy system, including system design, acquisition, installation, operation, upgrade, or replacement.

(4) Establish and validate Navy IA requirements and coordinate IA requirements that cross service boundaries with the Joint Staff in accordance with reference (c).

(5) Serve as the Resource Sponsor for Navy IA, following the guidelines of reference (af), for all DON (Navy, USMC, USCG and Military Sealift Command) cryptographic equipment based on DON priorities.

(6) Coordinate DON IA requirements for the DON Sensitive Compartmented Information (SCI)/Intelligence, and the DON portion of the DoD Intelligence Information System (DODIIS) with the Defense Intelligence Agency (DIA).

(7) Provide Navy representation to the Committee on National Security Systems, Sub-Committee on Telecommunications Security (TS) and Sub-Committee on Information Systems Security (SISS).

(8) Designate DAAs for information systems under Navy authority in accordance with references (c), (d), and (aa).

(9) Require registration of Navy IT systems and applications in the DON IT Registration Database in accordance with reference (f) and periodic guidance issued by DON CIO.

(10) Develop Navy IA education, training and awareness programs in accordance with DoD and DON policy, including annual IA, Internet security, privileged user, and DAA training.

(11) Require the training of personnel sufficient to assist the Navy in complying with the requirements of references (a) and (k), and related policies, procedures, and control techniques.

(12) Set policies and procedures to control access by foreign nationals to Navy-owned unclassified information, and Navy-owned and operated local area networks and information systems, in accordance with references (c), (d), (n), (o), (p), and (q).

(13) Implement standard formats specified in reference (d) to identify foreign nationals and contractors in all forms of communications owned and operated by the Navy, including e-mail, in accordance with reference (c).

(14) Provide for vulnerability mitigation, and an incident response and reporting capability, in accordance with reference (d).

(15) Review the Navy IA status annually to ensure it is fully consistent with the DON IA policy. Report these findings to DON CIO.

f. The Commandant of the Marine Corps shall:

(1) Ensure the integrity, confidentiality, authenticity,

availability, and non-repudiation of information and information systems supporting Marine Corps operations and assets.

(2) Develop and implement information assurance programs, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the Marine Corps. The Marine Corps IA programs shall contain the elements of a DoD Component IA Program as specified in enclosure (3) to reference (d).

(3) Ensure that information assurance is practiced throughout the life cycle of each Marine Corps system, including system design, acquisition, installation, operation, upgrade, or replacement.

(4) Establish and validate Marine Corps IA requirements and coordinate IA requirements that cross service boundaries with the Joint Staff in accordance with reference (c).

(5) Provide Marine Corps representation to the Committee on National Security Systems, Sub-Committee on Telecommunications Security (TS) and Sub-Committee on Information Systems Security (SISS).

(6) Designate DAAs for information systems under Marine Corps authority in accordance with references (c), (d), and (aa).

(7) Require registration of Marine Corps IT systems and applications in the DON IT Registration Database in accordance with reference (f) and periodic guidance issued by DON CIO.

(8) Develop Marine Corps IA education, training, and awareness programs in accordance with DoD and DON policy, including annual IA, internet security, privileged user, and DAA training.

(9) Require the training of personnel sufficient to assist the Marine Corps in complying with the requirements of references (a) and (k), and related policies, procedures, and control techniques.

(10) Set policies and procedures to control access by foreign nationals to Marine Corps-owned unclassified information, and Marine Corps-owned and operated local area networks and information systems, in accordance with references (c), (d), (n), (o), (p), and (q).

(11) Implement standard formats specified in reference (d) to identify foreign nationals and contractors in all forms of communications owned and operated by the Marine Corps, including e-mail, in accordance with reference (c).

(12) Provide for vulnerability mitigation, and an incident response and reporting capability, in accordance with reference (d).

(13) Review the Marine Corps IA status annually to ensure that it is fully consistent with the DON IA policy. Report these findings to DON CIO.

g. The Naval Inspector General shall carry out an annual independent evaluation of DON information assurance programs, in accordance with reference (a).

h. The Director, Naval Criminal Investigative Service shall:

(1) Contribute to CND by conducting investigations, operations, proactive programs, and related analyses of cyber incidents and targeting involving DON information systems.

(2) Assist and coordinate appropriate training for intrusion response personnel.

(3) Collect, track, and report on threats to DON information systems and disseminate this information to the DON CIO.

(4) Investigate fraud, waste, abuse and other criminal violations involving DON information systems.

(5) Maintain a staff skilled in the investigation of computer crime.

9. Action. All addressees shall implement this policy within their organizations.

10. Reports. The reports contained in this instruction are exempt from reports control by SECNAVINST 5214.2B.

Gordon England

Distribution List:
SNDL Parts 1 and 2
MARCORPS PCN 71000000000 and 71000000100

LIST OF ACRONYMS

AA/USN	Assistant for Administration, Office of the Under Secretary of the Navy
ASN	Assistant Secretary of the Navy
C&A	Certification and Accreditation
CAC	Common Access Card
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CMC	Commandant of the Marine Corps
CND	Computer Network Defense
CNO	Chief of Naval Operations
CNSS	Committee on National Security Systems (formerly the Committee on National Security Telecommunications and Information Systems Security)
COMSEC	Communications Security
COTS	Commercial-off-the-shelf
DAA	Designated Approving Authority
DCI	Director of Central Intelligence
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DODIIS	DoD Intelligence Information System
DON	Department of the Navy
FISMA	Federal Information Security Management Act
FIWC	Fleet Information Warfare Center
GIG	Global Information Grid
GOTS	Government-off-the-shelf
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection System
INFOCON	Information Operations Condition
INFOSEC	Information Systems Security
IT	Information Technology
JTF-GNO	Joint Task Force-Global Network Operations
MAC	Mission Assurance Category
MCNOSC	Marine Corps Network Operations and Security Command

NAVCIRT	Naval Computer Incident Response Team
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NSS	National Security Systems
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OMB	Office of Management and Budget
PK	Public Key
PKI	Public Key Infrastructure
RD&A	Research, Development, and Acquisition
SCI	Sensitive Compartmented Information
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SISS	Subcommittee for Information Systems Security
SSL	Secure Sockets Layer
STS	Subcommittee for Telecommunications Security
VAA	Vulnerability Analysis and Assessment
VPN	Virtual Private Network

Reference Location Table

Ref	Subject	Location
a	E-Government Act of 2002	http://www.doncio.navy.mil, under Policy and Guidance
b	CNSS Instruction 4009, National Information Systems Security Glossary, May 03	http://www.nstissc.gov/Assets/pdf/4009.pdf
c	DoDD 8500.1, Information Assurance (IA)	http://www.dtic.mil/whs/directives/
d	DoDI 8500.2, IA Implementation	http://www.dtic.mil/whs/directives/
e	DoDD 5000.1, the Defense Acquisition System	http://www.dtic.mil/whs/directives/
f	DoDI 5000.2, Operation of the Defense Acquisition System	http://www.dtic.mil/whs/directives/
g	Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, 17 Dec 03	http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
h	NSTISSD 500, Information Systems Security Education, Training, and Awareness, 25 Feb 93	http://www.nstissc.gov/Assets/pdf/nstissd_500.pdf
i	NSTISSI 4011, National Training Standard for Information Systems Security Professionals, 20 Jun 94	http://www.nstissc.gov/Assets/pdf/4011.pdf
j	NSTISSI 4012, National Training Standard for DAAs	http://www.nstissc.gov/Assets/pdf/4012.pdf
k	DoDD 8570.1, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/
l	SECNAVINST 5211.5D, DON Privacy Act Program	http://neds.nebt.daps.mil/Directives/dirindex.html
m	SECNAVINST 5720.47, DON Policy for Content of Publicly Accessible World Wide Web Sites	http://neds.nebt.daps.mil/
n	DoDD 5200.2, DoD Personnel Security Program	http://www.dtic.mil/whs/directives/
o	DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/
p	DoDD 5230.20, Visits, Assignments, and Exchanges of Foreign Nationals	http://www.dtic.mil/whs/directives/
q	DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations	http://www.dtic.mil/whs/directives/
r	DON CIO Guidance On IM/IT Inherently Governmental Functions, November 2001	http://www.doncio.navy.mil, under Policy and Guidance
s	DoDD O-8530.1, Computer Network Defense (CND)	DISA Web site: http://iase.disa.mil
t	DoDI O-8530.2, Support to CND	DISA Web site: http://iase.disa.mil
u	DoD CIO Memorandum of 7 Nov 00, Policy Guidance for Use of Mobile Code Technologies in DoD Information Systems	DISA Web site: http://iase.disa.mil

v	DoDD 8190.3, Smart Card Technology	http://www.dtic.mil/whs/directives/
w	Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/
x	OMB Circular A-130, Management of Federal Information Resources	http://www.whitehouse.gov/omb/circulars/index.html
y	DoDD 3020.26, Continuity of Operations (COOP) Policy	http://www.dtic.mil/whs/directives/
z	DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System	DISA Web site: http://iase.disa.mil
aa	DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)	http://www.dtic.mil/whs/directives/
ab	DCI Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems	http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm
ac	DoDD C-5200.5, Communications Security (COMSEC) (U)	DISA Web site: http://iase.disa.mil
ad	DoDD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dtic.mil/whs/directives/
ae	OMB Circular A-11, Preparation, Execution, and Submission of the Budget	http://www.whitehouse.gov/omb/circulars/index.html
af	OMB Memo M-00-07, Incorporating and Funding Security in Information Systems Investments	http://www.whitehouse.gov/omb/memoranda/index.html